

**PU030052 (JP2003249947) ON 8460**

- (19) Patent Agency of Japan (JP)
- (12) Official report on patent publication (A)
- (11) Publication number: 2003-249947
- (43) Date of publication of application: 05.09.2003
- (51) Int.Cl. H04L 12/56 H04L 12/46
- (21) Application number: 2002-046319
- (22) Date of filing: 22.02.2002
- (71) Applicant: Nippon Telegr & Teleph Corp <NTT>
- (72) Inventor: Kainuma Makoto, Takagi Koji, Yanagiya Mayumi, Tamura Toshihiko, Suzuki Kazuhiko
- (54) Title of the invention: Network system, method for setting intra-network identifier, intra-network information managing device, method for setting intra-network identifier of intra-network information managing device, radio access point, method for setting intra-network identifier of radio access point, edge switch, method for setting intra-network identifier of edge switch, program, and recording medium
- (57) Abstract:

Problem to be solved: To provide a network system for enabling a communication terminal to access another communication terminal within an optional IP service network or within the same network and enabling a user to select a service.

Solution: This network system sets a VLAN in a user unit among a radio access point or edge switch, a relay Layer2 switch and a router.

When a communication terminal is connected, an intra-network information managing device compares authentication information notified from the communication terminal with authentication information stored in an access authentication information management database, and sets a free VID as an intra-network identifier when the communication terminal is confirmed to be a legitimate user, and the radio access point or the edge switch registers the VID in a data frame sent from the communication terminal.

### **[Claims]**

#### **[Claim 1]**

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or the mentioned above edge switch, relay Layer2 switch that connects between the mentioned above routers, and an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network identifier management data base which manages VID which distinguishes a data frame for the mentioned above every communication terminal, the network system that it had and the mentioned above intra-network information management device, certification information notified

from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a registered user, and the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user, based on the mentioned above intra-network identifier management data base, 2nd means to choose vacant VID, to match vacant VID concerned and the mentioned above user ID, and to register with the mentioned above intra-network identifier management data base, the mentioned above VID selected by the mentioned above 2nd means, the mentioned above wireless access point, a registry request for making it register with the mentioned above edge switch or the mentioned above wireless access point or 3rd means to publish to the mentioned above edge switch and the mentioned above wireless access point, 4th means to cancel matching with the mentioned above VID registered into the mentioned above intra-network identifier management data base, and the mentioned above user ID, based on a release notice from the mentioned above edge switch, the mentioned above wireless access point, while an edge switch deletes setting out of the mentioned above VID at the time of 1st

means to register the mentioned above VID into a data frame from the mentioned above communication terminal and connection release of the mentioned above communication terminal, by a registry request from the mentioned above intra-network information management device, it has 2nd means to perform a release notice of the mentioned above VID to the mentioned above intra-network information management device.

[Claim 2]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch that connects between an edge switch and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network identifier management data base which manages a service identifier which recognizes VID which distinguishes a data frame for the mentioned above every communication terminal, and a connection destination IP service network, the above network system that it had and the mentioned above intra-network information management device, certification information notified from the mentioned above communication terminal at

the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a registered user, and the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user, based on the mentioned above intra-network identifier management data base, 2nd means to choose vacant VID, to match vacant VID concerned and the mentioned above user ID, and to register with the mentioned above intra-network identifier management data base, a notice of IP service ID showing IP service network name that wishes to connect is received from the mentioned above communication terminal, 3rd means to choose a vacant service identifier based on the mentioned above intra-network identifier management data base, to match the vacant service identifier concerned and the mentioned above IP service ID, and to register with the mentioned above intra-network identifier management data base, a registry request for making the mentioned above VID selected by the mentioned above 2nd and 3rd means, and the mentioned above service identifier register into a wireless access point or an edge switch, the mentioned above wireless access point or 4th means to publish to the mentioned above edge switch and the mentioned above wireless

access point or the mentioned above VID registered into the mentioned above intra-network identifier management data base based on a release notice from the mentioned above edge switch and the mentioned above user ID, including 5th means to cancel matching with the mentioned above service identifier and the mentioned above IP service ID, and the mentioned above wireless access point or 1st means by which an edge switch registers the mentioned above VID and the mentioned above service identifier into a data frame from the mentioned above communication terminal based on a registry request from the mentioned above intra-network information management device, while deleting setting out of the mentioned above VID and the mentioned above service identifier at the time of connection release of the mentioned above communication terminal, including 2nd means to perform a release notice of the mentioned above VID and the mentioned above service identifier to the mentioned above intra-network information management device, and the mentioned above router, it has a means to transmit a data frame from the mentioned above communication terminal to a router interface of IP service network matched with the mentioned above service identifier.

[Claim 3]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a

router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch that connects between an edge switch and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, and an intra-network identifier management data base which manages VID and a class of service identifier which distinguish a data frame for the mentioned above every communication terminal, the above network system that it had and the mentioned above intra-network information management device, certification information notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a registered user, and the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user, based on the mentioned above intra-network identifier management data base, 2nd means to choose vacant VID, to match vacant VID concerned and the mentioned above user ID, and to register with the mentioned above intra-network identifier management

data base, a notice of class of service ID showing a class of service name that wishes to connect is received from the mentioned above communication terminal, a vacant class of service identifier is chosen based on the mentioned above intra-network identifier management data base, the mentioned above VID selected by 3rd means to match vacant class of service identifier concerned and the mentioned above class of service ID and to register with the mentioned above intra-network identifier management data base, and the mentioned above 2nd and 3rd means, and the mentioned above class of service identifier, a wireless access point, a registry request for making it register with an edge switch, the mentioned above wireless access point, including 4th means to publish to the mentioned above edge switch, and the mentioned above wireless access point or the mentioned above VID registered into the mentioned above intra-network identifier management data base based on the mentioned above release notice from an edge switch and the mentioned above user ID, including 5th means to cancel matching with the mentioned above class of service identifier and the mentioned above class of service ID, and the mentioned above wireless access point or 1st means by which an edge switch registers the mentioned above VID and the mentioned above class of service identifier into a data frame from the mentioned above communication terminal based on a registry request from the mentioned above intra-network information management device,



while deleting setting out of the mentioned above VID and the mentioned above class of service identifier at the time of connection release of the mentioned above communication terminal, including 2nd means to perform a release notice of the mentioned above VID and the mentioned above class of service identifier to the mentioned above intra-network information management device, and the mentioned above wireless access point or an edge switch, the mentioned above relay Layer2 switch, and a router judge a priority of a data frame from the mentioned above communication terminal by the mentioned above class of service identifier, it has a means to choose an output port used as the destination of the data frame.

[Claim 4]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above wireless access point and the mentioned above routers, an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, and an intra-network identifier management data base which manages VID that distinguishes a data frame for the mentioned above every communication terminal, the above network system that it had and the mentioned above intra-

network information management device, certification information notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a registered user, and the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user, based on the mentioned above intra-network identifier management data base, 2nd means to choose vacant VID, to match vacant VID concerned and the mentioned above user ID, and to register with the mentioned above intra-network identifier management data base, 3rd means to publish a registry request for making the mentioned above VID selected by the mentioned above 2nd means register into the mentioned above wireless access point to the mentioned above wireless access point, after the mentioned above communication terminal moves to 2nd another wireless access point in the state where it connected with the 1st wireless access point, by the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user and user ID notified from the communication terminal concerned is the user ID in a life time, based on the mentioned above intra-network identifier management

data base, the same VID as VID which is used before the mentioned above communication terminal moved to the mentioned above 2nd access point, 4th means to publish a registry request for making it register with the mentioned above 2nd wireless access point to the mentioned above 2nd wireless access point, based on a release notice of the mentioned above VID from the mentioned above wireless access point, in the mentioned above life time, matching with the mentioned above VID currently held at the mentioned above intra-network identifier management data base and the mentioned above user ID is held, when the mentioned above life time is exceeded, including 5th means to cancel matching with the mentioned above VID and the mentioned above user ID, and the mentioned above wireless access point, while deleting setting out of the mentioned above VID at the time of 1st means to register the mentioned above VID into a data frame from the mentioned above communication terminal, and connection release of the mentioned above communication terminal, by a registry request from the mentioned above intra-network information management device, it has 2nd means to perform a release notice of the mentioned above VID to the mentioned above intra-network information management device.

[Claim 5]

A wireless access point connected with a communication terminal and the mentioned above communication terminal by radio, including or an edge switch connected

with the mentioned above communication terminal by cable, a router connected to IP service network, and the mentioned above wireless access point or relay Layer2 switch that connects between the mentioned above edge switch and the mentioned above routers, an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device that has an intra-network identifier management data base which manages VID which distinguishes a data frame for the mentioned above every communication terminal, and the mentioned above wireless access point or between the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, certification information with which are a setting method of an intra-network identifier in a network system which has set VLAN as a user unit, and it was notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal that the mentioned above intra-network information management device was, certification information corresponding to user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database is compared, the mentioned above intra-network information management device is the 1st step

that checks that the communication terminal concerned is a registered user, and the mentioned above 1st step. The 2nd step that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID, and is registered into the mentioned above intra-network identifier management data base when it is admitted that the communication terminal concerned is a registered user. The mentioned above intra-network information management device the mentioned above VID matched with the mentioned above user ID in the mentioned above 2nd step The mentioned above wireless access point or the 3rd step that publishes a registry request for making it register with the mentioned above edge switch to the mentioned above wireless access point or the mentioned above edge switch. The 4th step to which the mentioned above wireless access point or an edge switch registers the mentioned above VID into a data frame from the mentioned above communication terminal as an intra-network identifier by a registry request from the mentioned above intra-network information management device.

[Claim 6]

A setting method of the intra-network identifier according to claim 5 characterized by including the 5th step to which the mentioned above wireless access point or the mentioned above edge switch performs a release notice of the mentioned above VID to the mentioned

above intra-network information management device while deleting setting out of the mentioned above VID at the time of connection release of the mentioned above communication terminal, the 6th step of which the mentioned above intra-network information management device cancels matching with the mentioned above VID registered into the mentioned above intra-network identifier management data base and the mentioned above user ID based on the mentioned above wireless access point or a release notice from the mentioned above edge switch.

[Claim 7]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch that connects between an edge switch and the mentioned above routers. An access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network identifier management data base which manages a service identifier which recognizes VID which distinguishes a data frame for the mentioned above every communication terminal, and a connection destination IP service network. Certification information with which

are a setting method of provided with the above intra-network identifier, and it was notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal that the mentioned above intra-network information management device was, the 1st step that compares certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and checks that the communication terminal concerned is a registered user, when it is checked that the mentioned above intra-network information management device is the communication terminal concerned registered user by the mentioned above 1st step, the 2nd step that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID, and is registered into the mentioned above intra-network identifier management data base, the mentioned above intra-network information management device receives a notice of IP service ID showing IP service network name which wishes to connect from the mentioned above communication terminal, the 3rd step that chooses a vacant service identifier based on the mentioned above intra-network identifier management data base, matches the vacant service identifier concerned and the mentioned above IP service ID, and is registered into the mentioned above intra-network identifier management

data base, and the mentioned above intra-network information management device, the mentioned above VID with the mentioned above 2nd and 3rd selected steps, and the mentioned above service identifier, a wireless access point, a registry request for making it register with an edge switch or the mentioned above wireless access point or the 4th step published to the mentioned above edge switch and the mentioned above wireless access point or an edge switch has the 5th step that registers the mentioned above VID and the mentioned above service identifier into a data frame from the mentioned above communication terminal as an intra-network identifier based on a registry request from the mentioned above intra-network information management device.

[Claim 8]

A setting method of the intra-network identifier according to claim 7 characterized by including the 6th step to which the mentioned above wireless access point or the mentioned above edge switch performs a release notice of the mentioned above VID and the mentioned above service identifier to the mentioned above intra-network information management device while deleting setting out of the mentioned above VID and the mentioned above service identifier at the time of connection release of the mentioned above communication terminal. The mentioned above intra-network information management device, the mentioned above wireless access point or the 7th step of which



matching with the mentioned above VID registered into the mentioned above intra-network identifier management data base, the mentioned above user ID, and the mentioned above service identifier and the mentioned above IP service ID is canceled based on a release notice from the mentioned above edge switch.  
[Claim 9]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch that connects between an edge switch and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, and an intra-network identifier management data base which manages VID and a class of service identifier which distinguish a data frame for the mentioned above every communication terminal. Certification information with which are a setting method provided with the above intra-network identifier, and it was notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal that the mentioned above intra-network information management device was, the 1st step that compares

certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and checks that the communication terminal concerned is a registered user, when it is checked that the mentioned above intra-network information management device is the communication terminal concerned registered user by the mentioned above 1st step, the 2nd step that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID, and is registered into the mentioned above intra-network identifier management data base, the mentioned above intra-network information management device receives a notice of class of service ID showing a class of service name that wishes to connect from the mentioned above communication terminal, the 3rd step that chooses a vacant class of service identifier based on the mentioned above intra-network identifier management data base, matches vacant class of service identifier concerned and the mentioned above class of service ID, and is registered into the mentioned above intra-network identifier management data base, and the mentioned above intra-network information management device, the mentioned above VID with the mentioned above 2nd and 3rd selected steps, and the mentioned above class of service identifier, a wireless access point, a registry request for making it register with an edge switch or the

mentioned above wireless access point or the 4th step published to the mentioned above edge switch and the mentioned above wireless access point or an edge switch has the 5th step that registers the mentioned above VID and the mentioned above class of service identifier into an user-data frame as an intra-network identifier based on a registry request from the mentioned above intra-network information management device.

[Claim 10]

A setting method of the intra-network identifier according to claim 9 characterized by including the 6th step to which the mentioned above wireless access point or an edge switch performs a release notice of the mentioned above VID and the mentioned above class of service identifier to the mentioned above intra-network information management device while deleting setting out of the mentioned above VID and the mentioned above class of service identifier at the time of connection release of the mentioned above communication terminal, the mentioned above intra-network information management device, the mentioned above wireless access point or the 7th step of which matching with the mentioned above VID registered into the mentioned above intra-network identifier management data base, the mentioned above user ID, and the mentioned above class of service identifier and the mentioned above class of service ID is canceled based on the mentioned above release notice from an edge switch.

[Claim 11]

A communication terminal and a wireless access point connected with the mentioned above communication terminal by radio characterized by including the following, relay Layer2 switch which connects between a router connected to IP service network, and the mentioned above wireless access points and the mentioned above routers, an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device that has an intra-network identifier management data base which manages VID which distinguishes a data frame for the mentioned above every communication terminal, and the mentioned above wireless access point, a setting method of an intra-network identifier in the mentioned above router and a network system which are used for the mentioned above relay Layer2 switch with a network system and which has set up VLAN for every VID. Certification information it was notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal that the mentioned above intra-network information management device was. The 1st step that compares certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access

authentication information management database, and checks that the communication terminal concerned is a registered user. When it is checked that the mentioned above intra-network information management device is the communication terminal concerned registered user by the mentioned above 1st step, the 2nd step that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID, and is registered into the mentioned above intra-network identifier management data base. The 3rd step that publishes a registry request for the mentioned above intra-network information management device to make the mentioned above VID with the mentioned above 2nd selected step register into the 1st wireless access point to the mentioned above 1st wireless access point, when the mentioned above 1st wireless access point moves to 2nd another wireless access point from a state which the mentioned above communication terminal connected to the 1st wireless access point, while deleting setting out of the mentioned above VID, the 4th step that performs a release notice of the mentioned above VID to the mentioned above intra-network information management device, the mentioned above intra-network information management device based on a release notice of the mentioned above VID from the mentioned above 1st wireless access point, the 5th step of which matching with the mentioned above VID and the mentioned above user ID is canceled when matching with the mentioned

above VID currently held at the mentioned above intra-network identifier management data base and the mentioned above user ID is held and the mentioned above life time is exceeded in life time, after the mentioned above intra-network information management device moves to 2nd another wireless access point from a state which the mentioned above communication terminal connected to the 1st wireless access point, by the mentioned above 1st step. When it is checked that the communication terminal concerned is a registered user and the user ID concerned is the user ID in the mentioned above life time, based on the mentioned above intra-network identifier management data base, the same VID as VID which is used before the mentioned above communication terminal moved to the mentioned above 2nd access point, the 6th step that publishes a registry request for making it register with the 2nd wireless access point to the mentioned above 2nd wireless access point, and the mentioned above 2nd wireless access point by a registry request from the mentioned above intra-network information management device. The 7th step that registers the mentioned above VID into a data frame from a communication terminal with the user ID concerned as an intra-network identifier.

[Claim 12]

An intra-network information management device including a communication terminal, a wireless access point connected with the mentioned above

communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch which connects between the mentioned above edge switch and the mentioned above routers and the mentioned above wireless access point or between the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, it is an intra-network information management device in a network system which has set VLAN as a user unit, an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network information management device that has an intra-network identifier management data base which manages an intra-network identifier which distinguishes a data frame for the mentioned above every communication terminal, certification information notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a

registered user, and the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user, based on the mentioned above intra-network identifier management data base, choose a vacant intra-network identifier, and vacant identifier concerned intra-network and the mentioned above user ID are matched, the mentioned above intra-network identifier selected by 2nd means to register with the mentioned above intra-network identifier management data base, and the mentioned above 2nd means The mentioned above wireless access point or 3rd means to publish a registry request for making it register with the mentioned above edge switch to the mentioned above wireless access point or the mentioned above edge switch.

[Claim 13]

An intra-network information management device including a communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above wireless access point and the mentioned above routers, on the mentioned above wireless access point, the mentioned above router, and the mentioned above relay Layer2 switch. It is an intra-network information management device in a network system that is used with a network system and which has set up VLAN for every VID, an access authentication information management database that manages user



authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network information management device which has an intra-network identifier management data base which manages VID that distinguishes a data frame for the mentioned above every communication terminal, certification information notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, by 1st means to compare certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and to check that the communication terminal concerned is a registered user, and the mentioned above 1st means. 2nd means to choose vacant VID based on the mentioned above intra-network identifier management data base, to match vacant VID concerned and the mentioned above user ID, and to register with the mentioned above intra-network identifier management data base when it is checked that the communication terminal concerned is a registered user, 3rd means to publish a registry request for making the mentioned above VID selected by the mentioned above 2nd means register into the mentioned above wireless access point to the mentioned above wireless access point, after the mentioned above communication terminal moves to 2nd another wireless access point

from a state linked to the 1st wireless access point, by the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user and the user ID concerned is the user ID in a life time, based on the mentioned above intra-network identifier management data base, the same VID as VID that is used before the mentioned above communication terminal moved to the mentioned above 2nd access point, 4th means to publish a registry request for making it register with the 2nd wireless access point to the mentioned above 2nd wireless access point, based on a release notice of the mentioned above VID from the mentioned above wireless access point, in the mentioned above life time, 5th means to cancel matching with the mentioned above VID and user ID when matching with the mentioned above VID and user ID that are held at the mentioned above intra-network identifier management data base is held and the mentioned above life time is exceeded.

[Claim 14]

A wireless access point connected with a communication terminal and the mentioned above communication terminal by radio, including an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, and the mentioned above wireless access point or relay Layer2 switch that connects between the mentioned above edge switch and the mentioned above routers, an access authentication information management database that

manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device which has an intra-network identifier management data base which manages an intra-network identifier that distinguishes a data frame for the mentioned above every communication terminal, and the mentioned above wireless access point or between the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, certification information which is a setting method of an identifier of an intra-network information management device in a network system that has set VLAN as a user unit intra-network, and was notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal, certification information corresponding to user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database is compared, the 1st step that checks that the communication terminal concerned is a registered user, and the mentioned above 1st step, the 2nd step that chooses a vacant intra-network identifier based on the mentioned above intra-network identifier management data base, matches vacant identifier concerned intra-network and the mentioned above user ID, and is registered into the mentioned above intra-network

identifier management data base when it is admitted that the communication terminal concerned is a registered user, the 3rd step that publishes a registry request for making the mentioned above intra-network identifier matched with the mentioned above user ID register into the mentioned above wireless access point or the mentioned above edge switch in the mentioned above 2nd step to the mentioned above wireless access point or the mentioned above edge switch.

[Claim 15]

A communication terminal and a wireless access point connected with the mentioned above communication terminal by radio characterized by including the relay Layer2 switch that connects between a router connected to IP service network, and the mentioned above wireless access points and the mentioned above routers, an access authentication information management database which manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device which has an intra-network identifier management data base which manages VID which distinguishes a data frame for the mentioned above every communication terminal, and the mentioned above wireless access point, a setting method of an identifier of an intra-network information management device in the mentioned above router and a network system which are used for the mentioned above relay Layer2 switch with a network system and which

has set up VLAN for every VID of all the intra-network. Certification information notified from the mentioned above communication terminal at the time of a connection request of the mentioned above communication terminal. The 1st step that compares certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database, and checks that the communication terminal concerned is a registered user. When it is checked by the mentioned above 1st step that the communication terminal concerned is a registered user, the 2nd step that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID, and is registered into the mentioned above intra-network identifier management data base. The 3rd step that publishes a registry request for making the mentioned above VID with the mentioned above 2nd selected step register into the 1st wireless access point to the 1st wireless access point, based on a release notice of the mentioned above VID from the mentioned above 1st wireless access point, the 4th step of which matching with the mentioned above VID and the mentioned above user ID is canceled when matching with the mentioned above VID currently held at the mentioned above intra-network identifier management data base and the mentioned above user ID is held and the mentioned above life time is exceeded in

life time, after the mentioned above communication terminal moves to 2nd another wireless access point from a state linked to the mentioned above 1st wireless access point, by the mentioned above 1st step. When it is checked that the communication terminal concerned is a registered user and the user ID concerned is the user ID in the mentioned above life time, the 5th step that publishes a registry request for making the same VID as VID which is used before the mentioned above communication terminal moved to the mentioned above 2nd access point register into the 2nd wireless access point based on the mentioned above intra-network identifier management data base to the mentioned above 2nd wireless access point.

[Claim 16]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch which connects between the mentioned above edge switch and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, and an intra-network identifier management data base that manages an intra-network identifier which distinguishes

a data frame for the mentioned above every communication terminal, when it is admitted that it is the program provided with the above and the communication terminal concerned is a registered user, the 2nd procedure that chooses a vacant intra-network identifier based on the mentioned above intra-network identifier management data base, matches vacant identifier concerned intra-network and the mentioned above user ID, and is made to register into the mentioned above intra-network identifier management data base, in the mentioned above 2nd procedure, the mentioned above intra-network identifier made to choose the mentioned above wireless access point or an information management computer intra-network is made to perform the 3rd procedure of making a registry request for making it registering with the mentioned above edge switch publishing to the mentioned above wireless access point or the mentioned above edge switch.

[Claim 17]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above wireless access point and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, and an intra-network

identifier management data base which manages VID that distinguishes a data frame for the mentioned above every communication terminal, when it is checked that it is the program provided with the above and the communication terminal concerned is a registered user, the 2nd procedure that chooses vacant VID based on the mentioned above intra-network identifier management data base, matches vacant VID concerned and the mentioned above user ID and is made to register into the mentioned above intra-network identifier management data base, the 3rd procedure of making a registry request for making the mentioned above VID made choosing by the mentioned above 2nd procedure registering into the 1st wireless access point publishing to the 1st wireless access point, based on a release notice of the mentioned above VID from the mentioned above 1st wireless access point, the 4th procedure of making matching with the mentioned above VID and the mentioned above user ID canceling when matching with the mentioned above VID currently held at the mentioned above intra-network identifier management data base and the mentioned above user ID is held and the mentioned above life time is exceeded in life time, after the mentioned above communication terminal moves to 2nd another wireless access point from a state linked to the mentioned above 1st wireless access point, by the mentioned above 1st step. When it is checked that the communication terminal concerned is a registered user and the user ID concerned is the user ID in the mentioned above life



time, based on the mentioned above intra-network identifier management data base, the same VID as VID which is used before the mentioned above communication terminal moved to the mentioned above 2nd access point, the mentioned above information management computer intra-network is made to perform the 5th procedure of making a registry request for making it registering with the 2nd wireless access point publishing to the mentioned above 2nd wireless access point.

[Claim 18]

A communication terminal, an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, relay Layer2 switch which connects between the mentioned above edge switch and the mentioned above routers, an intra-network information management device including an edge switch and between the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, a means to register the mentioned above intra-network identifier into a data frame from a communication terminal with the mentioned above user ID by a registry request of an intra-network identifier that is an edge switch in a network system which has set VLAN as a user unit, and was matched with user ID from the mentioned above intra-network information management device.

[Claim 19] A communication terminal, an edge switch connected with the mentioned above communication

terminal by cable, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above edge switch and the mentioned above routers, and an intra-network information management device including the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, by a registry request of an intra-network identifier that is a setting method of an identifier of an edge switch in a network system that has set VLAN as a user unit intra-network, and was matched with user ID from the mentioned above intra-network information management device. A setting method of an identifier of an edge switch registering the mentioned above intra-network identifier into a data frame from a communication terminal with the mentioned above user ID intra-network.

[Claim 20]

A communication terminal, a computer that is connected with the mentioned above communication terminal by cable and functions as an edge switch, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above computer and the mentioned above routers, and an intra-network information management device including the mentioned above computer, the mentioned above relay Layer2 switch, and the mentioned above router, a computer in a network system that has set VLAN as a user unit, are an intra-network identifier a program made to set up, and the mentioned above program, a program making the

mentioned above computer perform a procedure of making the mentioned above intra-network identifier registering into a data frame from a communication terminal with the mentioned above user ID by a registry request of an intra-network identifier matched with user ID from the mentioned above intra-network information management device.

[Claim 21] A wireless access point including a communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to IP service network, relay Layer2 switch that connects between the mentioned above wireless access point and the mentioned above routers, including an intra-network information management device, and between the mentioned above wireless access point, the mentioned above relay Layer2 switch, and the mentioned above router to a user unit. Or it is a wireless access point in a network system that is used with a network system and which has set up VLAN for every VID, a means to register the mentioned above intra-network identifier into a data frame from a communication terminal with the mentioned above user ID by a registry request of an intra-network identifier matched with user ID from the mentioned above intra-network information management device.

[Claim 22] A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to

IP service network, relay Layer2 switch which connects between the mentioned above wireless access point and the mentioned above routers, and an intra-network information management device and the mentioned above wireless access point, the mentioned above relay Layer2 switch, and the mentioned above router to a user unit. Or it is a setting method of an identifier of a wireless access point in a network system that is used with a network system and which has set up VLAN for every VID of all the intra-network, a setting method of an identifier of a wireless access point intra-network registering the mentioned above intra-network identifier into a data frame from a communication terminal with the mentioned above user ID by a registry request of an intra-network identifier matched with user ID from the mentioned above intra-network information management device.

[Claim 23]

A communication terminal, a computer that is connected with the mentioned above communication terminal by radio, and functions as a wireless access point, a router connected to IP service network, relay Layer2 switch which connects between the mentioned above computer and the mentioned above routers, and an intra-network information management device, the mentioned above computer, the mentioned above relay Layer2 switch, and the mentioned above router to a user unit. A computer in a network system that is used with a network system and that has set up VLAN for every VID. An intra-network

identifier a program made to set up, and the mentioned above program, a program making a computer perform a procedure of making the mentioned above intra-network identifier registering into a data frame from a communication terminal with the mentioned above user ID by a registry request of an intra-network identifier matched with user ID from the mentioned above intra-network information management device.

[Claim 24] Claim 16, claim 17, claim 20 or a recording medium with which the program according to claim 23 was recorded.

### **[Detailed description of the invention]**

[0001]

[Field of the invention] In this invention, a setting method of a network system and an intra-network identifier, an intra-network information management device, the setting method of the identifier of an intra-network information management device intra-network, a wireless access point, a setting method of the identifier of the setting method of the identifier of a wireless access point intra-network, an edge switch, and an edge switch intra-network, the accessing means (wireless LAN art) from which plurality differs especially with respect to a program and a recording medium. In the information and telecommunications network that provides cable LAN art or IP service network systems with an available arbitrary communication terminal or other terminal same information and telecommunications intra-network is made possible, and it applies to the

public network system by the Ethernet art in which a communication terminal is able to choose a priority about data frame sending out arbitrarily and is related with effective art.

[0002]

[Description of the prior art] A communication terminal conventionally with the access system built with Ethernet art. When carrying out VLAN setting out for every connection, user authentication is performed at the time of communication terminal connection, the user ID and the wireless access point (next AP) that are user authentication information when it is able to check that he is a registered user by attestation or the thing for which VLAN setting out is performed using VID (Virtual LAN Identifier) matched with the physical port of the cable edge switch (next SW) or it has realized by setting up VLAN using VID matched with the MAC Address. About service selection nature, it has realized by using together protocols, such as PPP (Point-to-point Protocol).

[0003]

[Problems to be solved by the invention] However, when VLAN setting out was carried out for every connection by a method that was mentioned above, there was a problem that assignment of VID dynamic at the time of connection with a network (next an information and telecommunications network) could not be performed. Namely, (1) since VID in unused state cannot be utilized well according to the method that was mentioned above,

the problem that cannot use effectively VID (4094 pieces) which has restriction numerically, (2) VID and AP by the side of information and telecommunications network or since it is necessary to match matching of the physical port of the cable edge SW, VID by the side of an information and telecommunications network, and the MAC Address of a communication terminal and a user's utilizing environment is restricted by a utilizing location and the terminal, (3) when the problem and users to whom convenience gets worse wish connection with arbitrary IP service networks, when using PPP for service selection nature realization, before PPP Discovery Stage starts, in order for a communication terminal to share a plurality of broadcast domains, by the problem on that security levels, such as attack improper to other communication terminals and a spoofing failure of an IP address, deteriorate, and using PPP. State administrative traffic increased and there was a problem that makes a traffic resource intra-network useless.

[0004] IP service networks that are made in order that this invention may solve the problem of the mentioned above conventional technology and where the purpose of this invention has an arbitrary communication terminal or other communication terminal in the same network is made possible, a user makes service selection possible, and a communication terminal can choose a priority about data frame sending out arbitrarily, and it is in providing the network system by the Ethernet art in which the service durability at the time of movement is

securable by holding the same VID intra-network. Other purposes of this invention are to provide the setting method of the intra-network identifier in the mentioned above network system. Other purposes of this invention are to provide the setting method of the intra-network identifier in the intra-network information management device applied to the mentioned above network system, and an intra-network information management device. Other purposes of this invention are to provide the program for making the information management computer intra-network applied to the mentioned above network system perform the setting method of an intra-network identifier. Other purposes of this invention are to provide the access point applied to the mentioned above network system or an edge switch. Other purposes of this invention are to provide the program for making the access point applied to the mentioned above network system or the computer which functions as an edge switch perform the setting method of an intra-network identifier. Other purposes of this invention are to provide the recording medium with which the mentioned above program was recorded. The other purposes and the new feature are clarified with description and the accompanying drawing of this specification along this invention.

[0005]

[Means for solving the problem] It will be as follows if an outline of a typical thing is briefly explained among inventions indicated in this application. Namely, a



wireless access point by which this invention is connected with a communication terminal and the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, and the mentioned above wireless access point or relay Layer2 switch that connects between the mentioned above edge switch and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device that has an intra-network identifier management data base which manages VID that distinguishes a data frame for the mentioned above every communication terminal and the mentioned above wireless access point or between the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, certification information with which are the network system that has set VLAN as a user unit, and it was notified from the mentioned above communication terminal at the time of connection of a communication terminal that an intra-network information management device was, after comparing certification information stored in the mentioned above access authentication information management database and checking that the communication terminal concerned is a registered user

(next access authentication), VID in idle status is set up as an intra-network identifier, a wireless access point or an edge switch registers the mentioned above VID into a data frame from a communication terminal with the user ID concerned. At the time of connection release of a communication terminal, the mentioned above wireless access point or while the mentioned above edge switch deletes setting out of the mentioned above VID, a release notice of the mentioned above VID is performed to the mentioned above intra-network information management device, and the mentioned above intra-network information management device sets the VID concerned registered into the mentioned above intra-network identifier management data base as idle status.

[0006] According to this invention, it becomes possible to assign VID in an unused state, and it becomes possible to use effectively VID (4094 pieces) that has restriction numerically. VID and a wireless access point by the side of a network (information and telecommunications network) or since it is not necessary to match matching of a physical port of a cable edge switch, VID in a network, and a MAC Address of a communication terminal and a user's utilizing environment is restricted by neither a utilizing location nor terminal, it becomes possible to raise convenience. Since VID can be given to a user unit and a broadcast domain can be restricted with a wireless access point or a cable edge switch simultaneously with access authentication, it becomes possible to raise a security

level. An information management device with an access authentication information management database and an intra-network identifier management data base of the mentioned above intra-network communication terminal, a wireless access point or in order to perform remote attestation and a remote registration demand of an intra-network identifier to a cable edge switch, it becomes possible to reduce the User Information management and intra-network identifier management operation.

[0007] In this invention, in the mentioned above network system, at the time of connection of a communication terminal. Set up VID where an intra-network information management device cooperates with access authentication and which has it in idle status as an intra-network identifier, and a wireless access point or by registering the mentioned above VID into a data frame from a communication terminal in which an edge switch has the user ID concerned, for restricting a broadcast domain in addition, an intra-network information management device, a user sets up a service identifier that carries out connection hope and which is decided for every connection destination as an intra-network identifier, and a wireless access point or an edge switch registers the mentioned above service identifier into a data frame from a communication terminal with the user ID concerned, the mentioned above router transmits an user-data frame to a router interface of IP service network matched with the mentioned above service identifier.

At the time of connection release of a communication terminal, the mentioned above wireless access point or while deleting setting out of the mentioned above VID and the mentioned above service identifier, the mentioned above edge switch, a release notice of the mentioned above VID and the mentioned above service identifier is performed to the mentioned above intra-network information management device, and the mentioned above intra-network information management device sets the VID concerned registered into the mentioned above intra-network identifier management data base and the service identifier concerned as idle status. According to this invention, it becomes possible to raise service selection nature, without degrading security levels, such as attack improper to other communication terminals, and a spoofing failure of an IP address, in order not to share a broadcast domain among a plurality of communication terminals. Since administrative traffic does not occur, it becomes possible to use an intra-network traffic resource effectively.

[0008] In the mentioned above network system, this invention at the time of connection of a communication terminal sets up VID where an intra-network information management device cooperates with access authentication and which has it in idle status as an intra-network identifier, and a wireless access point or by registering the mentioned above VID into a data frame from a communication terminal in which an edge switch has the user ID concerned, for restricting a broadcast

domain in addition, an intra-network information management device, a user sets up a class of service identifier that carries out connection hope and which is decided for every class of service as an intra-network identifier, and a wireless access point or an edge switch registers the mentioned above class of service identifier into a data frame from a communication terminal with the user ID concerned, the mentioned above relay Layer2 switch and the mentioned above router judge a priority of the data frame concerned by the mentioned above class of service identifier, and choose an output port used as the destination of the data frame. At the time of connection release of a communication terminal, the mentioned above wireless access point or while deleting setting out of the mentioned above VID and the mentioned above class of service identifier, the mentioned above edge switch, a release notice of the mentioned above VID and the mentioned above class of service identifier is performed to the mentioned above intra-network information management device and the mentioned above intra-network information management device sets the VID concerned registered into the mentioned above intra-network identifier management data base, and the class of service identifier concerned as idle status. In order not to share a broadcast domain among a plurality of communication terminals according to this invention, it enables a communication terminal to choose a priority about data frame sending out arbitrarily, without degrading security levels, such as

attack improper to other communication terminals and a spoofing failure of an IP address.

[0009] A wireless access point by which this invention is connected with a communication terminal and the mentioned above communication terminal by radio, relay Layer2 switch that connects between a router connected to IP service network, and the mentioned above wireless access points and the mentioned above routers, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, including an intra-network information management device that has an intra-network identifier management data base which manages VID that distinguishes a data frame for the mentioned above every communication terminal, and the mentioned above wireless access point, the mentioned above router and the network system that are used for the mentioned above relay Layer2 switch with a network system and which has set up VLAN for every VID, after a communication terminal has connected with the 1st wireless access point, the mentioned above intra-network information management device, when it is checked that the communication terminal concerned is a registered user after moving to 2nd another wireless access point and the user ID concerned is the user ID in a life time, set up the same VID as VID that is used before the mentioned above communication terminal moved to the

mentioned above 2nd access point as an intra-network identifier, and the mentioned above wireless access point, the mentioned above VID is registered into a data frame from a communication terminal with the user ID concerned.

[0010] While deleting setting out of the mentioned above VID at the time of connection release of a communication terminal, the mentioned above wireless access point, performing a release notice of the mentioned above VID to the mentioned above intra-network information management device, and the mentioned above intra-network information management device between the mentioned above life time, when matching with the mentioned above VID and user ID that are held at the mentioned above intra-network identifier management data base is held and the mentioned above life time is exceeded, it is set as idle status of the mentioned above VID. By managing VID that cooperated with access authentication at the time of communication terminal connection, and was given, matching of user ID, and a connected state of a communication terminal according to this invention, since VID is certainly securable from the 1st wireless access point at the time of the 2nd radio access point, it becomes possible to secure connectivity at the time of movement. Since VID is eternal at the time of movement and service can be continued when having connected with a service network matched with VID, it becomes possible to raise a user's convenience.

[0011] This invention is a setting method of an intra-network identifier in the mentioned above network system. This invention is a setting method of an intra-network identifier in an intra-network information management device applied to the mentioned above network system, and an intra-network information management device. This invention is a setting method of a wireless access point applied to the mentioned above network system or an edge switch and a wireless access point or an intra-network identifier in an edge switch. An intra-network information management device, a wireless access point with which this invention is applied to the mentioned above network system or when a computer is used as an edge switch, it is the recording medium that recorded a program for performing a setting method of the mentioned above intra-network identifier and the program concerned on the computer concerned.

[0012]

[Embodiment of the invention] Next, with reference to drawings, an embodiment of the invention is described in details. In the complete diagram for describing an embodiment, what has the same function attaches identical codes and explanation of the repetition is omitted.

[Embodiment 1] Drawing 1 is a block diagram showing the outline composition of the public network system by the Ethernet art of the embodiment of the invention 1.



The public network system (next a public NW system) of this embodiment, it includes the relay Layer2 switch 4 that connects between the communication terminal 5, AP20 or cable edge SW21, the router 3 connected to the IP service network 9 and AP20 or cable edge SW21 and the routers 3, and the intra-network information management device 1. AP20 carries out direct housing of the communication terminal 5 by radio, namely, AP20 and the communication terminal 5 are connected by radio. Cable edge SW21 carries out direct housing of the communication terminal 5 by a cable and cable edge SW21 and a communication terminal are connected by the cable. The intra-network information management device 1 is provided with the access authentication information management database 6 that manages user authentication information for the communication terminal 5 to every user ID (identifier) identifiable to a meaning within a network, the intra-network identifier management data base 7 which manages VID that distinguishes a data frame for every communication terminal, AP20 or cable edge SW21 insert an identifier (VID) intra-network in the data frame (user-data frame) from a communication terminal based on the intra-network identifier registry request from the intra-network information management device 1. VLAN is set as the user unit between AP20 or cable edge SW21, the relay Layer2 switch 4 and the router 3.

[0013] Drawing 2 is a drawing showing handshaking of the public NW system of this embodiment. In drawing 2, the Challenge Handshake Authentication Protocol used at the time of access authentication is an access authentication protocol on Ethernet, such as IEEE 802.1x. Although this example explains using IEEE 802.1x, it is the same also at the access authentication protocol on other Ethernet. The communication terminal 5 of a public NW system connecting (L1 of drawing 2) based on the authentication procedure of IEEE 802.1x, a user notifies the user ID and certification information (password) for access authentication to the intra-network information management device 1 first (L2 of drawing 2). The intra-network information management device 1 carries out access authentication by comparing the user ID and certification information managed to the access authentication information management database 6 with the user ID and certification information which a user supplies (L3 of drawing 2). By access authentication, the certification information notified from the communication terminal 5 and the certification information over the user ID notified from the communication terminal 5 stored in the access authentication information management database 6 are in agreement, only when it is admitted that a user is a regular user of this network (next an information and telecommunications network), the intra-network information management device 1, based on the intra-network identifier management data base 7, VID (intra-

network identifier) for setting a broadcast domain as a user unit within Ethernet is chosen, vacant VID concerned and user ID are matched, and it registers with the intra-network identifier management data base 7. [0014] And the selected identifier (VID) concerned intra-network is notified to AP20 or cable edge SW21, and the registry request of user data frame is performed (L4 of drawing 2). AP20 that received the notice from the intra-network information management device 1 or cable edge SW21 is communication terminal-oriented network ports and the relay Layer2 switch 4 or the network ports which an information and telecommunications network turns are opened, and after inserting VID in the data frame from the communication terminal 5 concerned, two network ports are connected (L5 of drawing 2, L6). When the communication terminal 5 cancels connection with an information and telecommunications network (L7 of drawing 2), AP20 or cable edge SW21 eliminate VID set up for the communication terminal 5 concerned (L8 of drawing 2), and notifies it to the purport and the intra-network information management device 1 that were eliminated (L9 of drawing 2). The intra-network information management device 1 receives the notice of elimination of the intra-network identifier from AP20 or cable edge SW21, and cancels the correspondence relation of 1 to 1 between the relevance VID in an intra-network identifier management data base, and user ID (L10 of drawing 2).

By this, the VID concerned is vacant and is set up following connection that becomes usable. As explained above, in this embodiment, grant of VID that cooperated with user authentication becomes realizable.

[0015] Drawing 3 is a functional block diagram showing the internal configuration of the intra-network information management device 1. The intra-network information management device 1 is provided with the access authentication information management database 6, the intra-network identifier management data base 7, the intra-network identifier registry request / deletion request execution part 12, and the transmission and reception part 11. An intra-network identifier registry request / deletion request execution part 12 notifies an identifier (VID) intra-network to AP20 or cable edge SW21, when it is checked by access authentication that a user is a registered user of an information and telecommunications network, while performing access authentication. At the time of the connection release of the communication terminal 5, the correspondence relation of 1 to 1 between the relevance VID in an intra-network identifier management data base and user ID is canceled. The transmission and reception part 11 transmits and receives control information between AP20 or cable edge SW21 via an information and telecommunications network. Control information here means the information about access authentication, and an identifier (VID) intra-network.

Drawing 4 is a drawing showing the contents of the access authentication information management database 6 of this embodiment, and the intra-network identifier management data base 7. As shown on drawing 4 (A), the access authentication information management database 6, as User Information (certification information of user ID, a password, etc.) identifiable to a meaning is managed and the communication terminal 5 is shown on drawing 4 (B) information and telecommunications intra-network, the intra-network identifier management data base 7 manages user ID and VID given for every user ID.

[0016] Drawing 5 is a functional block diagram about AP20 of this embodiment or the intra-network identifier add function of cable edge SW21. AP20 or cable edge SW21 are provided with the data frame transmission and reception part 30, the Ethernet access authentication client function part 32, intra-network identifier registration / deletion execution part 31, and the transmission and reception part 33. The data frame transmission and reception part 30 publishes reception or the data frame from an information and telecommunications network for the data frame from the communication terminal 5 to the communication terminal 5. Intra-network identifier registration / deletion execution part 31 notifies the notice of connection release to the intra-network information management device 1, when the notice of an identifier (VID) intra-network is received from the intra-network information

management device 1, and the user data frame identifier concerned intra-network is inserted and connection of the communication terminal 5 is canceled. The access authentication client function part 32 transmits the user ID inputted from the communication terminal 5, and certification information to the intra-network information management device 1. The transmission and reception part 33 performs transmission and reception of the intra-network information management device 1 and control information by the router 3 (namely, information and telecommunications network). Control information here means the information about access authentication and an intra-network identifier.

[0017] [Embodiment 2] Since the public NW system by the Ethernet art of the embodiment of the invention 2 is the same as drawing 1, the graphic display of a system configuration is omitted. Drawing 6 is a drawing showing handshaking of the public NW system of this embodiment. In drawing 6, the Challenge Handshake Authentication Protocol used at the time of access authentication is an access authentication protocol on Ethernet, such as IEEE 802.1x. Although this example explains using IEEE 802.1x, it is the same also at the access authentication protocol on other Ethernet. The communication terminal 5 of this information and telecommunications network connecting (M1 of drawing 6) based on the authentication procedure of IEEE 802.1x, a user notifies the user ID and certification information for access authentication to the intra-

network information management device 1 first (M2 of drawing 6). The intra-network information management device 1 compares the user ID and certification information managed to the access authentication information management database 6 with the user ID and certification information that a user supplies, and carries out access authentication (M3 of drawing 6). Only when it is admitted by access authentication that a user is a regular user of this information and telecommunications network, the intra-network information management device 1, based on the intra-network identifier management data base 7, VID for setting a broadcast domain as a user unit within Ethernet is chosen, vacant VID concerned and user ID are matched, and it registers with the intra-network identifier management data base 7.

[0018] Based on the intra-network identifier management data base 7, IP service ID to which the mentioned above communication terminal 5 expresses IP service network name that wishes to connect, and a corresponding service identifier are chosen, the service identifier concerned and IP service ID are matched, and it registers with the intra-network identifier management data base 7. A user notifies IP service ID showing IP service network name to the intra-network information management device 1 by the communication terminal 5. VID of IEEE 802.1Q is used for this service identifier. And the selected intra-network identifier (VID, service identifier) is notified to AP20 or cable edge SW21, and

the registry request of user data frame is performed (M4 of drawing 6). AP20 that received the notice from the intra-network information management device 1 or in cable edge SW21, communication terminal-oriented network ports and information and telecommunications network-oriented network ports are opened, after inserting an intra-network identifier (VID, service identifier) (this is both VID of IEEE802.1Q) in the data frame from the communication terminal 5 concerned, two network ports are connected to it (M5 of drawing 6, M6). On the other hand, VID is set up fixed, and in AP20 or cable edge SW21, when an intra-network identifier is inserted, dynamic network paths will include relay Layer2SW4 information and telecommunications intra-network.

[0019] In the router 3, the router interface of IP service network unit is prepared, the mapping table of the router interface of a service identifier and IP service network unit is held, based on the service identifier in the network paths that mean a connection destination IP service network, an user-data frame is transmitted to IP service network of which it was required at the time of a connection request. When the communication terminal 5 cancels connection with an information and telecommunications network (M7 of drawing 6), AP20 or cable edge SW21 is notified to the purport intra-network information management device 1 that was set up for the communication terminal 5 concerned and which eliminated and (M8 of drawing 6) eliminated the



intra-network identifier (VID, service identifier) (M9 of drawing 6). The intra-network information management device 1 AP20 or the notice of elimination of the intra-network identifier from cable edge SW21 is received and the correspondence relation of 1 to 1 between the relevance VID in an intra-network identifier management data base and user ID and the correspondence relation of 1 to 1 between IP service ID and a service identifier are canceled (M10 of drawing 6). By this, the intra-network identifier (VID, service identifier) concerned is vacant, and is set up following connection becomes usable. As explained above, according to this embodiment, it becomes possible to raise the convenience of the communication terminal 5 by guaranteeing service selection nature and security reservation simultaneously in the information and telecommunications network by Ethernet.

[0020] Since the internal configuration of the information management device 1 of this embodiment intra-network is the same as drawing 3, the detailed explanation is omitted. However, in this embodiment the intra-network identifier registry request / deletion request execution part 12 of the intra-network information management device 1, when it is checked by access authentication that a user is a registered user of an information and telecommunications network, the mentioned above VID and service identifier as an intra-network identifier AP20 or while notifying to cable edge SW21, at the time of the connection release of the

communication terminal 5, the intra-network identifier to which it corresponds in the intra-network identifier management data base 7 is set as idle status. Although the graphic display of the contents of the access authentication information management database 6 of this embodiment is omitted, the access authentication information management database 6 of this embodiment manages User Information (certification information, such as user ID and a password) identifiable to a meaning for the communication terminal 5 with an information and telecommunications network like drawing 4 (A). Drawing 7 is a drawing showing the contents of the intra-network identifier management data base 7 of this embodiment. As shown on drawing 7, the intra-network identifier management data base 7 manages user ID, the IP services ID and VID, and a service identifier. Since the composition about AP20 of this embodiment or the intra-network identifier add function of cable edge SW21 is the same as drawing 5, detailed explanation is omitted.

[0021] [Embodiment 3] Since the public NW system by the Ethernet art of the embodiment of the invention 3 is the same as drawing 1, the graphic display of a system configuration is omitted. Drawing 8 is a drawing showing handshaking of the public NW system of this embodiment. In drawing 8, the Challenge Handshake Authentication Protocol used at the time of access authentication is an access authentication protocol on Ethernet, such as IEEE 802.1x.

Although this example explains using IEEE 802.1x, it is the same also at the access authentication protocol on other Ethernet. The communication terminal 5 of this information and telecommunications network connecting (N1 of drawing 8) based on the authentication procedure of IEEE 802.1x, a user notifies the user ID and certification information for access authentication to the intra-network information management device 1 first (N2 of drawing 8). The intra-network information management device 1 compares the user ID and certification information managed to the access authentication information management database 6 with the user ID and certification information that a user supplies, and carries out access authentication (N3 of drawing 8). Only when it is admitted by access authentication that a user is a regular user of this information and telecommunications network, the intra-network information management device 1, based on the intra-network identifier management data base 7, VID for setting a broadcast domain as a user unit within Ethernet is chosen, vacant VID concerned and user ID are matched and it registers with the intra-network identifier management data base 7.

[0022] Based on the intra-network identifier management data base 7, use the priority tag of IEEE 802.1Q. The class of service identifier matched with class of service ID that specifies the class of service that a user wishes is chosen, the class of service identifier concerned and class of service ID are matched, and it

registers with the intra-network identifier management data base 7. A user notifies class of service ID that specifies the class of service which a user wishes to the intra-network information management device 1 by the communication terminal 5. And an identifier (VID, class of service identifier) intra-network is notified to AP20 or cable edge SW21 and the registry request of user data frame is performed. AP20 that received the notice from the intra-network information management device 1 or cable edge SW21 opens communication terminal-oriented network ports and information and telecommunications network-oriented network ports, after inserting an identifier (VID, class of service identifier) intra-network in the data frame from the communication terminal 5 concerned, two network ports are connected to it (N5 of drawing 8, N6). Here, VID is VID of IEEE 802.1Q and a class of service identifier is a priority tag of IEEE 802.1Q.

[0023] On the other hand, the router 3, relay Layer2SW4, and AP20 or when an user-data frame is received, cable edge SW21 by a class of service identifier. The priority of the data frame concerned is judged and a class of service is provided for every communication terminal by mapping in one of the available CoS (Class of Service) in the output port used as the destination of the data frame. When the communication terminal 5 cancels connection with an information and telecommunications network (N7 of drawing 8), AP20 or cable edge SW21 is notified to the

purport intra-network information management device 1 which was set up for the communication terminal 5 concerned and which eliminated and (N8 of drawing 8) eliminated the intra-network identifier (VID, class of service identifier) (N9 of drawing 8). The intra-network information management device 1 AP20 or the notice of elimination of the intra-network identifier from cable edge SW21 is received, and the correspondence relation of 1 to 1 between the relevance VID in an intra-network identifier management data base and user ID and the correspondence relation of 1 to 1 between class of service ID and a class of service identifier are canceled (N10 of drawing 6). By this, the identifier (VID, class of service identifier) concerned intra-network is vacant, and is set up following connection that becomes usable. As explained above, according to this embodiment, it becomes possible to raise the convenience of the communication terminal 5 by guaranteeing class of service selectivity and security reservation simultaneously in the information and telecommunications network by Ethernet.

[0024] Drawing 9 is a drawing showing an example of grant of the class of service identifier of this embodiment. As shown on drawing 9, a class of service identifier (priority TAG) can be given in 0-8 steps. Here, priority means that the user-data frame concerned is ability ready for sending ahead of other data frames. For example, as shown on drawing 9, when priority TAG is set up in two steps and priority TAG is 0 (priority

TAG=0), it gives priority and transmits, and when priority TAG is 1 (priority TAG=1), it transmits by a best effort. Since the internal configuration of the information management device 1 of this embodiment intra-network is the same as drawing 3, the detailed explanation is omitted. However, in this embodiment the intra-network identifier registry request / deletion request execution part 12 of the intra-network information management device 1, when it is checked by access authentication that a user is a registered user of an information and telecommunications network, the mentioned above VID and class of service identifier as an intra-network identifier AP20 or while notifying to cable edge SW21, at the time of the connection release of the communication terminal 5, the intra-network identifier to which it corresponds in the intra-network identifier management data base 7 is set as idle status. Although the graphic display of the contents of the access authentication information management database 6 of this embodiment is omitted, the access authentication information management database 6 of this embodiment manages User Information (certification information, such as user ID and a password) identifiable to a meaning for the communication terminal 5 with an information and telecommunications network like drawing 4 (A). Drawing 10 is a drawing showing the contents of the intra-network identifier management data base 7 of this embodiment.

As shown on drawing 10, the access authentication information management database 6 manages user ID, the classes of service ID and VID, and a class of service identifier. Since the composition about AP20 of this embodiment or the intra-network identifier add function of cable edge SW21 is the same as drawing 5, detailed explanation is omitted.

[0025] [Embodiment 4] Drawing 11 is a block diagram showing the outline composition of the public NW system by the Ethernet art of the embodiment of the invention 4. The public NW system of this embodiment includes the relay Layer2 switch 4 that connects between the communication terminal 5, AP20, the router 3, and AP20 and the routers 3, and the intra-network information management device 1. AP20 carries out direct housing of the communication terminal 5 by radio, namely, AP20 and the communication terminal 5 are connected by radio. Here, the intra-network information management device 1 is provided with the access authentication information management database 6 that manages user authentication information for the communication terminal 5 to every user ID (identifier) identifiable to a meaning within a network, the intra-network identifier management data base 7 that manages VID which distinguishes a data frame for every communication terminal, AP20 inserts an identifier (VID) intra-network in the data frame (user-data frame) from a communication terminal based on the intra-network identifier registry request from the intra-

network information management device 1. In this embodiment, VLAN is set to the router 3 and the relay Layer2 switch 4 fixed for every VID of all the used for AP20 by the public NW system by Ethernet art. For example, in using VID of 0-1000, it sets up TAG of 1000.

[0026] The case where it moves to another AP20 (next the 2nd AP) in the state where it connected with the mentioned above AP20 (next the 1st AP) is explained. Drawing 12 is a drawing showing handshaking of the public NW system of the embodiment of the invention 4, and is a drawing showing handshaking when the communication terminal 5 moves. In drawing 12, the Challenge Handshake Authentication Protocol used at the time of access authentication is an access authentication protocol on Ethernet, such as IEEE 802.1x. Although this example explains using IEEE 802.1x, it is the same also at the access authentication protocol on other Ethernet. About the procedure that the communication terminal 5 connects with an information and telecommunications network, since it is the same as the mentioned above Embodiment 1, about the procedure concerned, it is next called the procedure of Embodiment 1. If the mentioned above communication terminal 5 moves to the AP20 to 1st 2nd AP20, cutting will take place by the physical layer of radio access (O1 of drawing 12). Thus, the procedure of Embodiment 1 is again started by the 2nd AP20 subordinate (O2 of drawing 12).



The period that can reuse VID with the information management device 1 same after cutting of the communication terminal 5 intra-network in that case (the following and life time) are held, and when the difference of the disconnection time of the communication terminal 5 that it has left to the intra-network identifier management data base 7, and the present time is in life time, the correspondence relation of 1 to 1 between user ID and VID is held (O3 of drawing 12).

[0027] By the case where it is admitted by the access authentication of 2nd AP20 that the communication terminal 5 concerned is a registered user after the communication terminal 5 moving, when it is the user ID that is during the mentioned above life time, the intra-network information management device 1 carries out the registry request of the same VID as VID using VID of IEEE 802.1Q that is used last time to the 2nd AP20 based on the intra-network identifier management data base 7 (O4 of drawing 12). In the 2nd AP20 that received the notice from the intra-network information management device 1. Communication terminal-oriented network ports and information and telecommunications network-oriented network ports are opened and after inserting an identifier (VID of IEEE 802.1Q) intra-network in the data frame from the communication terminal 5 concerned, two network ports are connected (O5 of drawing 12, O6). In the case (O7 of drawing 12) where connection of the communication terminal 5 is

canceled, the 2nd AP20 setting out of VID deleting (O8 of drawing 12) the release notice of VID is performed to the mentioned above intra-network information management device 1 (O9 of drawing 12). Based on a release notice, the intra-network information management device 1 starts a timer, and the inside of the life time, when matching with the relevance VID and user ID in the intra-network identifier management data base 7 is held and life time is exceeded, matching with the relevance VID in an intra-network identifier management data base and user ID is canceled (O10 of drawing 12). In this embodiment, when connecting with an information and telecommunications network newly from the communication terminal 5, handshaking is the same as the mentioned above Embodiment 1.

[0028] Since the internal configuration of the information management device 1 of this embodiment intra-network is the same as drawing 3, the detailed explanation is omitted. Although the graphic display of the contents of the access authentication information management database 6 of this embodiment is omitted, the access authentication information management database 6 of this embodiment manages User Information (certification information, such as user ID and a password) identifiable to a meaning for the communication terminal 5 with an information and telecommunications network like drawing 4 (A). Drawing 13 is a drawing showing the contents of the intra-network identifier management data base 7 of this

embodiment. As shown on drawing 13, the intra-network identifier management data base 7 manages user ID, VID, and a connected state recording flag. The connected state recording flag shown on drawing 13 serves as one, when the communication terminal 5 is connected to the information and telecommunications network, and it is set to OFF within the mentioned above life time. Since the composition about the intra-network identifier add function of AP20 of this embodiment is the same as drawing 5, detailed explanation is omitted. In the mentioned above explanation, the intra-network information management device 1, as for performing by computer, AP20 or cable edge SW21 are also possible, and in that case or the intra-network information management device 1 or the setting method of AP20 or the identifier of cable edge SW21 intra-network is performed when a computer executes the program stored in the hard disk in a computer, etc. This program is supplied by downloading from CD-ROM or a network. As mentioned above, as for this invention, although the invention made by this invention person was concretely explained based on the mentioned above embodiment, it is needless to say for it to be able to change variously in the range that is not limited to the mentioned above embodiment and does not deviate from the gist.

[0029]

[Effect of the invention] It will be as follows if the effect acquired by the typical thing among the inventions indicated in this application is explained briefly.

(1) According to this invention, it becomes possible to use effectively VID that has restriction numerically and to raise a user's convenience, and to aim at intra-network management operation reduction.

(2) According to this invention, it becomes possible to realize service selection nature that does not degrade a security level and does not make an intra-network traffic resource useless and selectivity of the class of service of a CoS level.

(3) According to this invention, it becomes possible to realize service durability at the time of movement of a communication terminal.

### **[Brief description of the drawings]**

[Drawing 1] is a block diagram showing the outline composition of the public network system by the Ethernet art of the embodiment of the invention 1.

[Drawing 2] is a drawing showing handshaking of the public network system of the embodiment of the invention 1.

[Drawing 3] is a functional block diagram showing the outline composition of the intra-network information management device 1 shown on drawing 1.

[Drawing 4] is a drawing showing the contents of the access authentication information management database and the intra-network information identifier management data base of the embodiment of the invention 1.

[Drawing 5] is a functional block diagram showing the intra-network identifier add function of the cable edge SW and AP shown on drawing 1.

[Drawing 6] is a drawing showing handshaking of the public network system of the embodiment of the invention 2.

[Drawing 7] is a drawing showing the contents of the intra-network identifier management data base of the embodiment of the invention 2.

[Drawing 8] is a drawing showing handshaking of the public network system of the embodiment of the invention 3.

[Drawing 9] is a drawing showing the example of class of service realization in the embodiment of the invention 3.

[Drawing 10] is a drawing showing the contents of the intra-network identifier management data base of the embodiment of the invention 3.

[Drawing 11] is a block diagram showing the outline composition of the public network system by the Ethernet art of the embodiment of the invention 4.

[Drawing 12] is a drawing showing handshaking of the public network system of the embodiment of the invention 4.

[Drawing 13] is a drawing showing the contents of the intra-network identifier management data base of the embodiment of the invention 4.

### **[Description of numerals]**

1... An intra-network information management device,  
3... A router, 4... Relay Layer2 switch,  
5... A communication terminal,  
6... An access authentication information management database,  
7... Intra-network identifier management data base,  
9... IP service network,  
11, 33... A transmission and reception part,  
12... Intra-network identifier registry request / deletion request execution part,  
20... A wireless access point, 21... A cable edge switch,  
30... A data frame transmission and reception part,  
31... Intra-network identifier registration / deletion execution part,  
32... Access authentication client function part

[Procedure correction]

[Filing date] 2002.02.27

[Amendment 1]

[Document to be amended] Specification

[Item to be amended] Claim 12

[Method of amendment] Change

[Proposed amendment]

**[Claim 12]**

**A wireless access point connected with a communication terminal and the mentioned above communication terminal by radio or an edge switch connected with the mentioned above communication terminal by cable, a router connected to IP service network, the mentioned above wireless access point or relay Layer2 switch that connects between the mentioned above edge switch and the mentioned above routers, an intra-network information management device in a network system that has set VLAN as a user unit between the mentioned above wireless access point or the mentioned above edge switch, the mentioned above relay Layer2 switch, and the mentioned above router, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network identifier management data base that manages an intra-network identifier that distinguishes a data frame for the mentioned above every communication terminal, 1st means to compare certification information notified from the mentioned above communication terminal with certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database at the time of a connection request of the mentioned above communication terminal and to check that the communication terminal concerned is a**

registered user, when it is checked by the mentioned above 1st means that the communication terminal concerned is a registered user, 2nd means to choose a vacant intra-network identifier based on the mentioned above intra-network identifier management data base, to match vacant identifier concerned intra-network and the mentioned above user ID and to register with the mentioned above intra-network identifier management data base, the mentioned above intra-network identifier selected by the mentioned above 2nd means, the mentioned above wireless access point or an intra-network information management device including 3rd means to publish a registry request for making it register with the mentioned above edge switch to the mentioned above wireless access point or the mentioned above edge switch.

[The amendment 2]

[Document to be amended] Specification

[Item to be amended] Claim 13

[Method of amendment] Change

[Proposed amendment]

[Claim 13]

A communication terminal, a wireless access point connected with the mentioned above communication terminal by radio, a router connected to IP service network, a relay Layer2 switch that connects between the mentioned above wireless access point and the mentioned above routers, an intra-network information

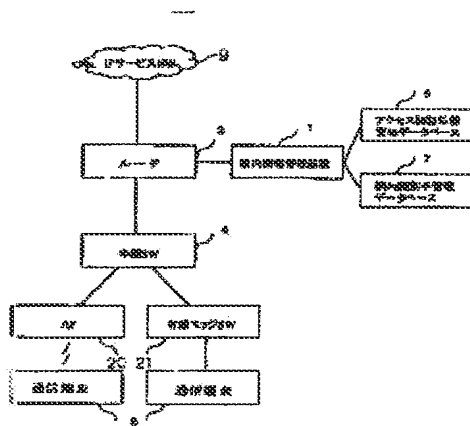


management device in the mentioned above wireless access point, the mentioned above router and a network system that are used for the mentioned above relay Layer2 switch with a network system and that has set up VLAN for every VID, an access authentication information management database that manages user authentication information for the mentioned above communication terminal for every user ID identifiable to a meaning within a network, an intra-network identifier management data base that manages VID that distinguishes a data frame for the mentioned above every communication terminal, 1st means to compare certification information notified from the mentioned above communication terminal with certification information over user ID notified from the mentioned above communication terminal stored in the mentioned above access authentication information management database at the time of a connection request of the mentioned above communication terminal, and to check that the communication terminal concerned is a registered user, 2nd means to choose vacant VID based on the mentioned above intra-network identifier management data base, to match vacant VID concerned and the mentioned above user ID and to register with the mentioned above intra-network identifier management data base when it is checked by the mentioned above 1st means that the communication terminal concerned is a registered user, 3rd means to publish a registry request for making the mentioned above VID selected by the

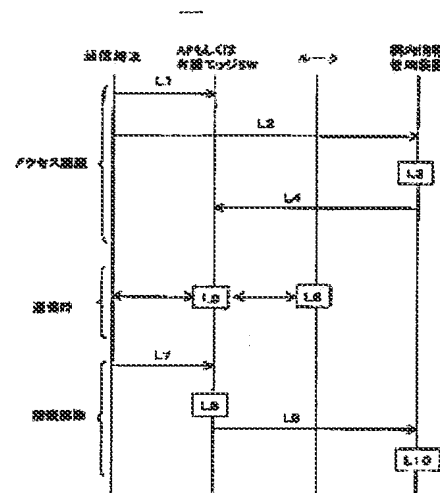
mentioned above 2nd means register into the mentioned above wireless access point to the mentioned above wireless access point, after the mentioned above communication terminal moves to 2nd another wireless access point from a state linked to the 1st wireless access point, by the mentioned above 1st means. When it is checked that the communication terminal concerned is a registered user and the user ID concerned is the user ID in a life time, 4th means to publish a registry request for making the same VID as VID that is used before the mentioned above communication terminal moved to the mentioned above 2nd access point register into the 2nd wireless access point based on the mentioned above intra-network identifier management data base to the mentioned above 2nd wireless access point, based on a release notice of the mentioned above VID from the mentioned above wireless access point, in the mentioned above life time, an intra-network information management device including 5th means to cancel matching with the mentioned above VID and user ID when matching with the mentioned above VID and user ID that are held at the mentioned above intra-network identifier management data base is held and the mentioned above life time is exceeded.



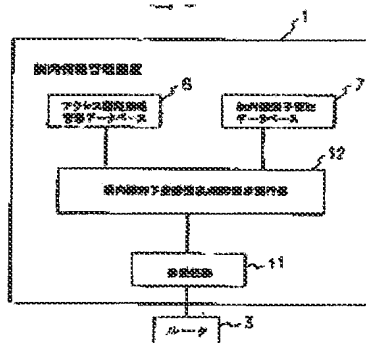
Drawing 1



Drawing 2



Drawing 3



Drawing 4

(A) アクセス制御装置データベース

ユーザID	パスワード

(B) 網内制御装置データベース

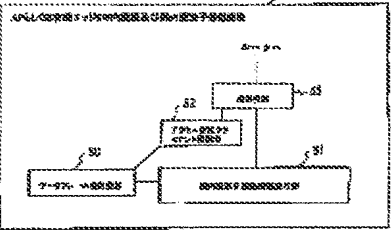
ユーザID	IPアドレス

Drawing 7

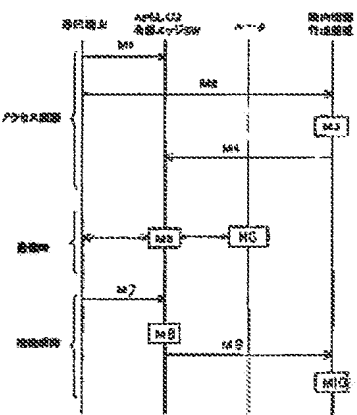
データベース

ユーザID	パスワード	IP	アクセス権

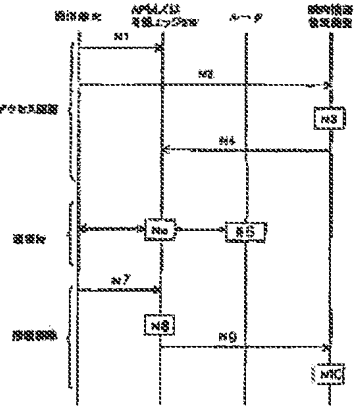
Drawing 5



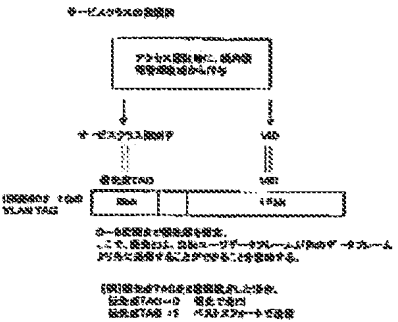
Drawing 6



Drawing 8



Drawing 9



Drawing 13

図13の回路図

電源	接地	制御ユニット